

Decision Logs

Decision Logs Notarized

1. The Mandate for Verifiable Causality

In any economic or safety-critical system, the operational integrity of an action is inseparable from the verifiable justification *for* that action. Traditional binary systems, which operate on a ``text{proceed/fail}`` basis, are architecturally incapable of providing this linkage. Their logs are *post-facto*, recording effects—such as a database error or a completed transaction—rather than the *ante-facto* causes, inputs, and authorizations that constitute the decision itself.

This "evidentiary deficit" creates an environment where accountability is a matter of forensic archaeology rather than immediate inspection. It permits "policy laundering," "memory-holing," and "retrospective reconstruction," whereby an institution may, in the event of an adverse outcome, invent a rationale that suits its post-facto interests.

Decision Logs as the Genesis of Causality

Ternary Logic (TL) remedies this deficit through the Decision Log (DL), the Fourth Pillar. A Decision Log is not a "log" in the traditional, passive sense; it is the *genesis* of the action itself. It is a "complete narrative," documenting the "who, what, when, where, why, and how" of any material operation. It captures the complete "justification for intent" as a rich, structured dataset *before* that intent is permitted to become an action.

The "No Log = No Action" Covenant

The Fourth Pillar is enforced by an inviolable covenant: ``text{No Log = No Action}``. This mandate inverts the traditional audit model. Instead of an action occurring, which *might* create a log, the TL framework mandates that the *creation* of a complete, well-formed, and signed DL is the *atomic prerequisite* for the action's execution.

This makes ``ex ante`` transparency and accountability an unavoidable architectural property, not an ``ex post`` operational goal.

Eliminating Retrospective Reconstruction

The "No Log = No Action" covenant, combined with the immutability of the DL artifact, programmatically eliminates bad-faith historical revisionism:

- **Preventing Retrospective Reconstruction:** An institution cannot "reconstruct" a favorable narrative for a past decision. The DL *is* the one and only narrative, and it was created ``ex ante`` (before the fact).

- **Preventing Policy Laundering:** An operator cannot justify a failed action by claiming they were operating on data or policies that were not available at the time. The DL immutably binds the action to the *exact* data inputs and models used at the millisecond of intent.
- **Preventing Memory-Holing:** An operator cannot delete an unfavorable record. The DL is sealed to the Immutable Ledger (Pillar 2) and externally notarized by Anchors (Pillar 8). Under TL, "even aborted actions remain part of institutional memory".

Non-Repudiable Accountability Across Jurisdictions

The Decision Log serves as the primary enforcement mechanism for the entire framework. Its existence, or lack thereof, creates a "reverse burden of proof".

This establishes a powerful legal doctrine: the "rebuttable presumption of negligence or system design failure". In the event of an adverse outcome (e.g., a market crash, a sanctions violation), the burden of proof shifts *from* the regulator *to* the institution. The institution is not asked to "explain what happened"; it is required to *produce the Decision Log*.

- If the DL is absent, incomplete, or ill-formed, negligence is presumed.
- If the DL is present and well-formed, it provides a complete, mathematical defense of the actions taken.

This "weaponizes transparency", providing a sovereign piece of cryptographic evidence that supersedes borders and jurisdictions. A regulator in any nation does not need to trust an institution's internal reports; they simply request the DL.

2. Core Function and Immutable Lifecycle

The Decision Log is the evidentiary artifact that is created, evaluated, and sealed during the lifecycle of any TL-governed operation.

The Fourth Pillar Invocation

The 4th Pillar is invoked *before* the 3rd Pillar (Epistemic Hold). It is the first step in the operational flow. An actor (human or automated) proposes a `+1 (\text{Intent})` action. This intent is immediately halted at the first gate, which demands compliance with the "No Log = No Action" covenant. At this moment, the system generates the DL in a "pre-commit" state.

Standardized Structure of the Decision Log

The DL is not a simple text file; it is a "rich, structured dataset" designed for forensic, regulatory, and automated analysis. Its fields are rigidly defined to capture the full causal chain of the decision.

Table 1: Decision Log Standardized Structure

Field	Data Type	Description	Purpose (Forensic Substrate)
DL_UUID	Hash	A unique, non-repudiable identifier for this log entry.	Evidentiary linkage.
Timestamp	Millisecond UTC	Immutable timestamp of '+1 (\text{Intent})' creation.	Establishes "what was known, when."
Initiator_ID	Pseudonym	Pseudonymous identifier of the actor (human or bot) initiating the request.	Accountability (See Section 6).
Authorizer_ID	Pseudonym	Pseudonymous identifier(s) of all actors authorizing the action.	Accountability (See Section 6).
Action_Payload	Struct	The proposed action itself (e.g., transaction details, command).	Defines the '+1 (\text{Intent})'.
Data_Inputs	{Hash:Value}	A hashed map of all data inputs used to inform the decision.	Prevents data substitution (reconstruction).
Models_Invoked	{Hash:Version}	Hashed identifiers of all models/rules used.	Proves <i>which</i> logic was used (See Section 7).
Confidence_Score	Float	The resulting confidence score from the model(s).	Provides objective measure of certainty.
Risk_Flags	Array	All automated risk flags triggered by inputs.	Provides verifiable proof of risk awareness.

Field	Data Type	Description	Purpose (Forensic Substrate)
Mandate_Check_v5	Hash	Proof of Economic Rights & Transparency check.	Enforces compliance (Pillar 5).
Mandate_Check_v6	Hash	Proof of Sustainable Capital Allocation check.	Enforces compliance (Pillar 6).
Hold_State	Enum	`\text{NULL}` at creation. Updated to `\text{TRIGGERED}` if Hold occurs.	Lifecycle tracking.
Hold_Reason	String	Reason for the `0` (\text{Epistemic Hold}).	Causal link to deliberation.
Hold_Deliberation	Text/Hash	Log of actions taken during the Hold (e.g., "new data queried").	Proves due diligence during pause.
Final_State	Enum (`+1`, 0, -1`)	The final resolved state (`+1` Proceed, -1` Halt).	Binds intent to final outcome.
Signature	Crypto. Sig.	Cryptographic signature binding all fields.	Ensures integrity and non-repudiation.

The Ternary Lifecycle (`+1` / 0 / -1`)

The DL artifact moves through three distinct states:

1. **`+1` (\text{Intent})**: **DL Creation Before the Epistemic Hold.** The action is proposed. The DL is instantly generated, and the fields from DL_UUID through Mandate_Check_v6 are populated. The log is now in a "pre-commit" state, its intent declared.
2. **`0` (\text{Hold})**: **The DL Frozen as the Subject of Deliberation.** If uncertainty is high or mandate checks fail, the 3rd Pillar, Epistemic Hold, is triggered. The DL artifact is now *frozen*. Its initial Data_Inputs cannot be altered. This frozen log becomes the *subject* of the deliberation. Any new data queried or human reviews conducted are appended to the Hold_Deliberation field, not used to overwrite the original context.

3. **`+1 / -1 (\text{Resolution})`**: **Binding the Final Outcome to Evidence.** The Hold concludes with a final decision: **`+1 (\text{Proceed})`** or **`-1 (\text{Halt})`**. The **Final_State**, **Hold_Reason**, and **Hold_Deliberation** fields are populated, and the entire record is cryptographically signed.

Absolute Immutability

Once the DL is signed, it is absolutely immutable. No edits, overwrites, or "updated reasons" are possible. No addenda can be attached (though a *new* action, with its *own* DL, may reference a prior DL). This ensures the "chronologically sound history" of the system is absolute and non-repudiable.

3. Sequential Interaction with the Eight Pillars Framework

The Decision Log is the core artifact that is passed sequentially through the Ternary Logic architectural framework. Its journey creates the "full causal chain" of evidence.

1. **Pillar 4 (Decision Logs)**: An action (**`+1`** Intent) is proposed. The "No Log = No Action" covenant is enforced, and the DL is created.
2. **Goukassian Principle**: The newly created DL, specifically its **Action_Payload** and **Initiator_ID** fields, immediately faces its "constitutional boundaries". It is checked against the absolute prohibitions: "No Spy" and "No Weapon".
3. **Pillars 5 & 6 (Mandates)**: The DL is checked for compliance with the Economic Rights & Transparency and Sustainable Capital Allocation mandates. The DL itself serves as the auditable proof that these verifications occurred.
4. **Pillar 3 (Epistemic Hold)**: If the action's confidence score is low, data is conflicting, or any Mandate/Principle check fails, the Epistemic Hold (**`0`**) is triggered. The DL, created at step 1, is now the central package under review, and the **Hold_Deliberation** field is activated.
5. **Pillar 2 (Immutable Ledger)**: After the Hold resolves to a final **`+1`** or **`-1`**, the *entire, completed* DL—capturing the "initial +1 intent, the 0 Hold deliberation, and the final +1 or -1 outcome"—is recorded on the Immutable Ledger. It is now "cryptographically sealed".
6. **Pillar 7 (Hybrid Shield)**: The sealed DL, now residing on the Ledger, is protected by the Hybrid Shield. This Pillar is a cryptographic and legal layer that "manages access", balancing the "public's right to verify with the institution's need to protect sensitive information".
7. **Pillar 8 (Anchors)**: Finally, the *hash* of the sealed DL is "anchored to public blockchains". This provides "decentralized, time-stamped verification". This final step serves as the ultimate backstop against a catastrophic, collusive internal attack. Even if an institution attempted to destroy its *entire* internal ledger, the public anchor chain would provide non-repudiable proof of the missing DLs, instantly invoking the "rebuttable presumption of negligence".

4. Integration with the Ternary Logic Governance Triad

The Decision Log is the "cryptographically verifiable source of truth" upon which the entire TL Governance Triad operates. This triad—comprising the Technical Council, Stewardship Custodians, and Smart Contract Treasury —has no authority to alter DL content; its sole function is to interpret this evidence.

- **Technical Council:** This body "maintains cryptographic standards" and "technical health". Its primary function is to audit the *protocol*, not the *operators*. It uses DLs for conformance testing, initiating test actions and forensically analyzing the resulting DLs to ensure they are well-formed, cryptographically sound, and compliant with the standardized schema (Table 1).
- **Stewardship Custodians:** This body acts as the judiciary, "enforcing foundational principles" and "ruling on revocation". When an alleged "No Spy" violation occurs, the DL is the *only* evidence reviewed. The Custodians analyze the Initiator_ID, Data_Inputs, and Action_Payload fields to make a determination. A revocation of an operator's certification *must* be justified by a chain of non-compliant DLs.
- **Smart Contract Treasury:** This body "funds approved development". It uses DLs for automated, verifiable milestone payments. A development team's contract is funded by the Treasury. The contract's terms are automated: to prove a milestone is complete, the new code must run in a sandbox and successfully execute a task that *produces a valid, well-formed DL*. The Treasury's smart contract validates the DL hash and automatically releases the funds.

Foundational Mandates

The Governance Triad is bound by the same mandates that govern the DL's creation:

1. **No Log = No Action:** The prerequisite for all existence in the system.
2. **No Spy, No Weapon:** The absolute prohibitions of the Goukassian Principle. The DL is the evidence that this line was not crossed.
3. **No Switch Off:** The mandate that makes accountability non-negotiable. An operator cannot "pull the plug" on the logging protocol to avoid generating an incriminating DL during an adverse event. The logging framework is an uninterruptible, critical service. To terminate it is the ultimate violation, invoking an immediate and "rebuttable presumption of negligence" for the entire duration of the outage.

5. The Dual-Lane Architecture: Evidence and Action

A core challenge in high-stakes environments is the conflict between performance and integrity. High-performance trading, for example, requires sub-300ms execution, while high-integrity logging ("No Log = No Action") implies a slow, blocking cryptographic write.

The Ternary Logic framework resolves this conflict via a "Dual-Lane Architecture," which separates high-speed execution from high-integrity evidence.

- **Lane 1: The Action Lane (High-Performance):** This is the execution environment, targeting sub-300ms operations.
- **Lane 2: The Evidence Lane (High-Integrity):** This is the DL, Immutable Ledger, and Anchor protocol.

The "No Log = No Action" mandate serves as the *atomic commit* that links them. The flow is as follows:

1. ($T=0\text{ms}$) Action proposed in Lane 1.
2. ($T=50\text{ms}$) Lane 2 instantly creates the DL in-memory, signs it, and generates its final hash (DL_Hash_123).
3. ($T=51\text{ms}$) This DL_Hash_123 "commit" signal is sent to Lane 1.
4. ($T=52\text{ms}-299\text{ms}$) Lane 1 executes the action, its "why" now immutably locked.
5. ($T=300\text{ms}+$) Lane 2, in an asynchronous process, completes the full, heavier cryptographic sealing of the DL onto the Immutable Ledger and Anchors.

This write-ahead model satisfies both requirements. The action is *not* blocked by the full DLT write, only by the near-instant in-memory signature, ensuring both speed and non-repudiable integrity.

6. GDPR, Privacy, and Evidentiary Continuity

A second core conflict is that between the *immutability* of the ledger and the *right to erasure* mandated by privacy regimes such as GDPR. It is architecturally impossible to delete data from an immutable ledger.

The solution is to ensure that Personal Identifiable Information (PII) *never touches the ledger*.

1. **Pseudonymization:** When a user interacts, the system generates a Pseudonym_ID (e.g., user_hash_123).
2. **DL Stripping:** The Decision Log is created, but the Initiator_ID field contains *only* user_hash_123 .
3. **The Link:** The mapping ($\text{user_hash_123} \rightarrow \text{PII}$) is stored in a separate, *mutable*, and highly secure database managed by the **Hybrid Shield (Pillar 7)**.
4. **Sealing:** The DL, containing *only* the pseudonym and the non-personal "why" of the action, is sealed on the Immutable Ledger.
5. **Erasure Request:** A user invokes their Right to Erasure. The system accesses the Hybrid Shield's *mutable* database and deletes the link.

6. **Evidentiary Continuity:** The Immutable Ledger is untouched. The DL, `\dots\text{action taken by user_hash_123}\dots``, remains permanently. The "why" is preserved for regulators, but *who* `\text{user_hash_123}`` was is now permanently and cryptographically "forgotten."

7. Trade Secrets and Ephemeral Key Rotation (EKR)

A third conflict exists between transparency ("models used") and confidentiality (a bank's proprietary risk model). An institution's core IP cannot be written to any log.

The DL's Models_Invoked field (Table 1) stores only a *hash* of the model, not the logic.

Verification is handled by Ephemeral Key Rotation (EKR) *during* an Epistemic Hold.

1. **Execution:** An action uses a proprietary model. The DL logs `\text{model_invoked: hash_of_model_v3}``.
2. **Epistemic Hold ('0'):** An audit is triggered , perhaps by Stewardship Custodians.
3. **EKR Initiated:** The **Hybrid Shield (Pillar 7)** generates a *one-time ephemeral key pair*.
4. **Decryption:** This key is shared *only* with the institution's secure enclave and the auditor's verification tool *for the duration of the Hold window*. This allows the auditor to inspect and test the model's logic.
5. **Hold Resolution:** The Hold ends.
6. **Keys Vanish:** The ephemeral key is destroyed.

The result is a "proof of existence" that remains on the ledger. The *why* (the model's internal logic) was verifiable *at the time* but vanishes, protecting the trade secret while ensuring accountability.

8. Detailed Examples Across Sectors

The following examples demonstrate the full operational flow of the Decision Log through the Ternary Logic framework.

1. Finance / Anti-Money Laundering (AML)

- **+1 (\text{Intent})`:** A bank's automated system initiates a \$5.2 million cross-border transfer.
- **\text{DL Creation}`:** A DL is created (Dual-Lane commit). Action_Payload: 5.2M_USD. Data_Inputs: hash_of_KYC_files, risk_score_78. Models_Invoked: hash_of_risk_model_v4.
- **'0 (\text{Epistemic Hold})`:** The **Economic Rights & Transparency Mandate (Pillar 5)** fails, triggering an immediate Hold. *Hold Reason:* "Data provenance failure." The Data_Inputs (KYC file hash) do not match the hash on file for the receiver, signaling a sanctions-list or identity mismatch.

- **`-1 (\text{Resolution})`**: A human compliance officer is alerted, reviews the frozen DL, confirms the mismatch, and issues a **`-1 (\text{Halt})`**.
- **`\text{Ledger / Anchor}`**: The *complete* DL (intent, mandate failure, human review, final refusal) is sealed and anchored. The bank now possesses a non-repudiable "rebuttable presumption" defense, proving it stopped a high-risk transaction.

2. Supply Chain (High-Value Pharmaceuticals)

- **`+1 (\text{Intent})`**: An automated logistics system proposes to reroute a 2-ton shipment of refrigerated medicines.
- **`\text{DL Creation}`**: DL created. Action_Payload: Reroute_via_Vendor_B. Data_Inputs: sensor_temp_2C, gps_location, port_strike_alert.
- **`0 (\text{Epistemic Hold})`**: The system triggers a Hold. *Hold Reason*: "Data conflict." The Data_Inputs are in conflict: the weather feed for the *new* route shows a 4-hour window at 35°C, which would destroy the shipment.
- **`+1 (\text{Resolution})`**: *Deliberation*: The system automatically queries a "challenger" model to find a *third* route. The third route is verified as safe. The system resolves to **`+1 (\text{Proceed})`** with the new, verified route.
- **`\text{Ledger / Anchor}`**: The DL is sealed. Regulators (e.g., FDA) can audit this single DL and see the full "intellectual history" of the decision: the initial intent, the detected risk, the deliberation, and the safe resolution.

3. Healthcare / Medical AI (Diagnostics)

- **`+1 (\text{Intent})`**: A hospital's AI diagnostic system analyzes an oncology scan and proposes: Diagnosis: No Malignancy.
- **`\text{DL Creation}`**: DL created. Initiator_ID: AI_Model_G-45. Data_Inputs: hash_of_DICOM_scan, patient_pseudonym_9a8f. Models_Invoked: hash_of_diagnostic_model_v7. Confidence_Score: 51.2%.
- **`0 (\text{Epistemic Hold})`**:** The system instantly triggers a Hold. *Hold Reason*: "Confidence score (51.2%) below 85% threshold." The AI knows it is uncertain.
- **`+1 (\text{Resolution})`**: *Deliberation*: The system escalates to a human. A radiologist (logged via Authorizer_ID) reviews the scan, concurs, and signs off on the **`+1 (\text{Proceed})`**.
- **`\text{Ledger / Anchor}`**: The DL is sealed. This record is non-repudiable medico-legal proof of due diligence. It respects the *Right to Erasure* (per the Section 6 model) while providing a permanent, immutable record for liability defense.

4. Autonomous Robotics (Industrial Safety)

- **`+1 (\text{Intent})`**: A 10-ton industrial robot moves to perform a high-torque weld.
- **`\text{DL Creation}`**: DL created. Initiator_ID: robot_arm_004. Action_Payload: Weld_Cycle_XYZ. Data_Inputs: lidar_scan_clear, camera_feed_clear.

- **`0 (\text{Epistemic Hold})`**: The **Goukassian Principle** triggers a Hold. *Hold Reason*: "Potential 'Weapon' state." A micro-vibration (a new Data_Input) conflicts with the 'clear' sensor feeds. The system cannot be 100% certain a human is not in the cell.
- **`+1 (\text{Resolution})`**: *Deliberation*: The arm is frozen. The vibration is identified as a benign, known harmonic. The "Weapon" flag is cleared. The system resolves to **`+1 (\text{Proceed})`**.
- **`\text{Ledger / Anchor}`**: The DL is sealed, creating a perfect, sub-second safety log and a non-repudiable defense against a negligence claim.

5. Energy Grid Management (Critical Infrastructure)

- **`+1 (\text{Intent})`**: An automated grid-balancing system proposes to shunt 500MW of power from Substation A to B to prevent a brownout.
- **`\text{DL Creation}`**: DL created. Action_Payload: Shunt_500MW_A_to_B. Data_Inputs: demand_forecast_high, substation_B_load_80%.
- **`0 (\text{Epistemic Hold})`**: The **Sustainable Capital Allocation Mandate (Pillar 6)** fails, triggering a Hold.
- **`-1 (\text{Resolution})`**:** *Hold Reason*: "Missing 'veracity' data". The data for Substation A's *transformer-age-and-stress-test* is missing. The system *cannot* verify that "A" can handle the load-shift without catastrophic failure. It refuses the action: **`-1 (\text{Halt})`**.
- **`\text{Ledger / Anchor}`**: The DL is sealed. This record proves the system *prevented* a potential infrastructure collapse by enforcing the Mandate. It chose a minor brownout over a catastrophic failure and has the non-repudiable mathematical proof of *why*.

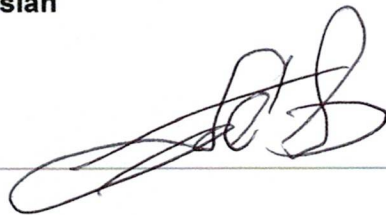
Execution and Witnessing

Declaration Execution

Document: **Decision_Logs_Notarized.md**

Declarant: **Lev Goukassian**

Signature:



Date:

NOV 13/2025

ORCID: **0009-0006-5966-1243**

Email: leogouk@gmail.com

Witness Requirements

Two witnesses attest that the declarant:

1. Had full mental capacity at the time of signing,
2. Executed this document voluntarily,
3. Had their identity verified.

Witness 1

Name:

Jalen Smith

Signature:

J Smith

Date:

11/13/25

Relationship:

UPS Store Employee

Witness 2

Name:

Akouri Ekore

Signature:



Date:

11/13/25

Relationship:

Ups store employee

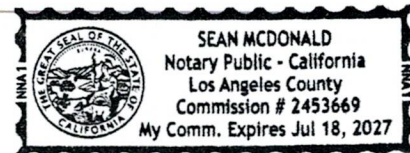
Notarization

Notary Public:

Sean McDonald

Signature and Seal:





Date:

11/13/25

Commission Expires:

July 18, 2027

Chain of Custody Metadata

chain_of_custody:

document: Decision_Logs_Notarized.md

created_by: Lev Goukassian (ORCID: 0009-0006-5966-1243)

signed_at: 2025-11-12T14:00-08:00

notarized_at: 2025-11-12T15:00-08:00

file_hash: 7a62607bb2bcd52dd365530e5f1147cad547b02a63f22b3a39994e66ce56075e

anchor_targets:

- Bitcoin (OpenTimestamps)
- Ethereum AnchorLog
- Polygon AnchorLog

repository: <https://github.com/FractonicMind/TernaryLogic>

version: 1.0.0-notarized

verification_method: sha256 + opentimestamps

2025-11-13 (2.6)